Crypto, Key Protection, and Mobility in Windows

Sean Finnegan

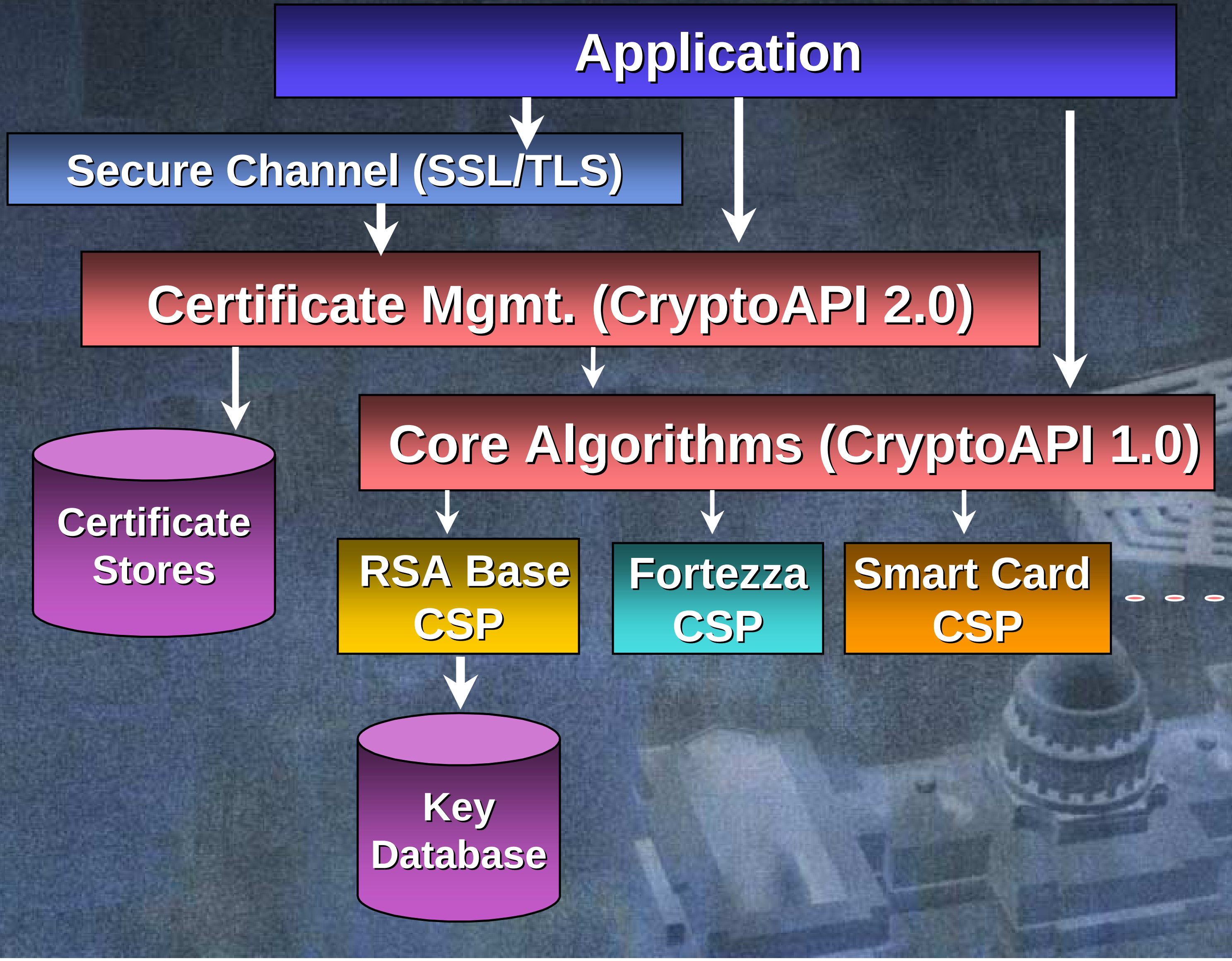
Security Program Manager

Microsoft Government Systems

Crypto Support In Windows

- Microsoft Crypto API has been an integral part of Windows since ~1996
- Ship vehicle varies but functionality the same on all platforms
  - Updated via Internet Explorer on Win9x
  - Updated via Service Packs on NT and Windows 2000

CryptoAPI Framework



Application

Secure Channel (SSL/TLS)

Certificate Mgmt. (CryptoAPI 2.0)

Certificate Stores

Core Algorithms (CryptoAPI 1.0)

RSA Base CSP

Fortezza CSP

Smart Card CSP

- - -

Key Database

Private Key Protection

- Protected Storage Service (PSTORE) has managed keys for CSPs in Windows since NT4 SP3/IE4
  - Provides memory management for keys in non-paged memory
  - Takes care of key protection for storage
  - Keys stored encrypted in HKEY_CURRENT_USER registry hive
- Windows 2000 introduced the Data Protection API (DPAPI)
  - Provides same services as PSTORE but lets the CSP store the protected keys
  - RSA CSPs store keys as a file in the user's profile directory

"C:\Documents and Settings\*userid*\Application Data\Microsoft\Crypto\RSA"

How Private Keys Are Protected

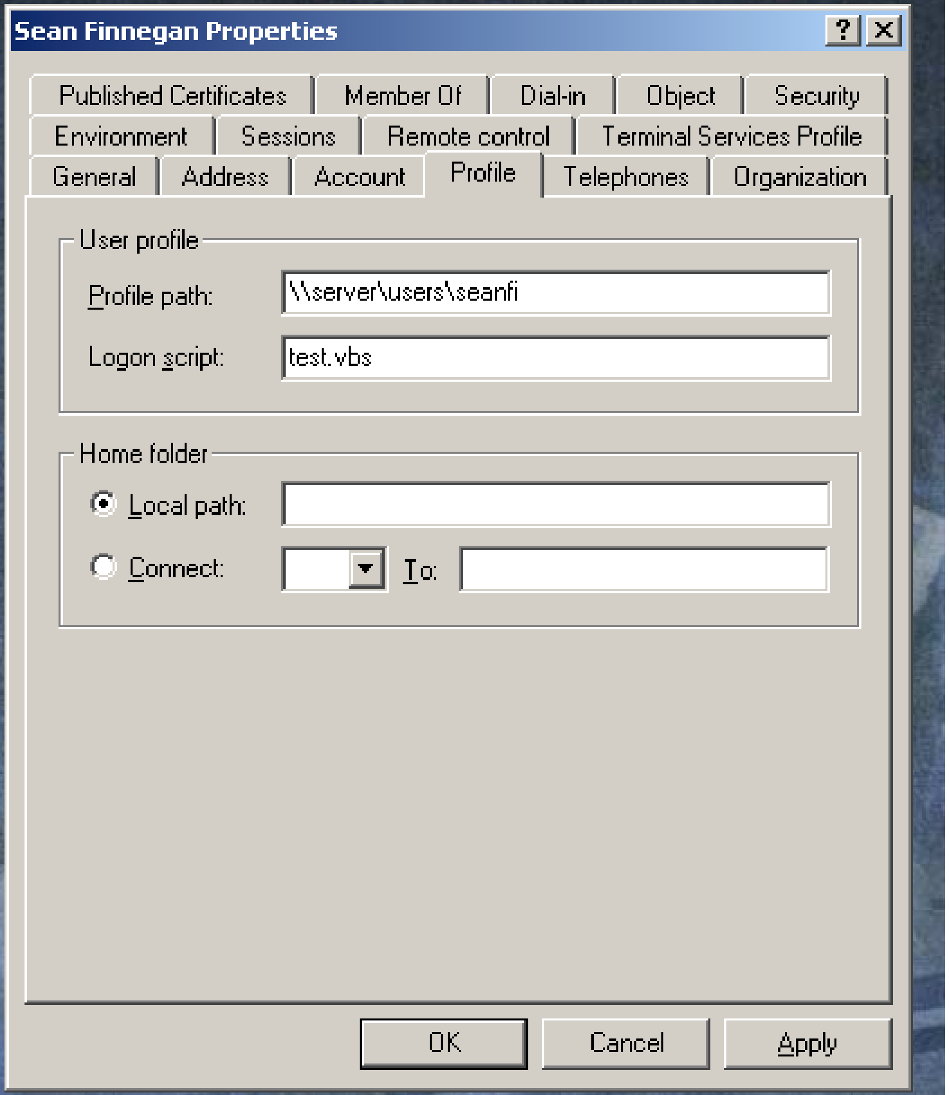
- A per user master key is created at first logon
- User master key changed every 60 days
  - Only new data encrypted with new key
- Two copies of user master key are stored in the user’s profile
  - One is encrypted using user 160-bit RC4 key
    - Key created by SHA HMAC of user logon credentials and a random*
  - Second is a blinded version encrypted by the DC master key
    - Used in the event of password reset

Secondary PK Protection

- Keys generated by default cannot be exported from PSTORE/DPAPI
  - The flag CRYPT_EXPORTABLE must be set at generation/import time to enable key export
- CSPs may also implement the CRYPT_USER_PROTECTED flag to provide a second level of key protection
  - The flag is set on the key at generation or import time only
  - When set the user is prompted for an optional second password to access private key

Key Mobility

- Windows 9x/NT/2000 all support roaming user profiles when in a domain environment
- Per user configuration on domain accounts
- Profile copied from server at logon and updated at logoff
  - Includes entire profile directory and HCU registry hive
- Registry setting to control profiles caching



Sean Finnegan Properties

User profile

Profile path: \\server\users\seanfi

Logon script: test.vbs

Home folder

● Local path:

○ Connect: To:

http://www.microsoft.com/security

http://www.microsoft.com/windows2000

seanfi@microsoft.com